DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340-5100

FEB 15 2019

U-19-3000/FAC-2A1 (FOIA)

Ms. Emma Best
MuckRock News
DEPT MR 57507
411ª Highland Ave
Somerville, MA 02144-2516

Dear Ms. Best:

This responds to your Freedom of Information Act (FOIA) request, dated July 5, 2005, that you submitted to the Defense Intelligence Agency (DIA) for information concerning color reproductions of any posters, flyers, brochures, bulletins or other graphic designs intended to remind employees and visitors of security practices or warn them about potential security failings and vulnerabilities to include any OPSEC posters. I apologize for the delay in responding to your request. DIA continues its efforts to eliminate the large backlog of pending FOIA requests. In order to properly respond, it was necessary to consult with another office within the agency.

A search of DIA's systems of records located nine documents (26 pages) responsive to your request.

Upon review, I have determined that some portions of the nine documents (26 pages) must be withheld in part from disclosure pursuant to the FOIA. The withheld portions are exempt from release pursuant to Exemption 3 of the FOIA, 5 U.S.C. § 552 (b)(3). Exemption 3 applies to information specifically exempted by a statute establishing particular criteria for withholding. The applicable statute is 10 U.S.C. § 424. Statute 10 U.S.C. § 424 protects the identity of DIA employees, the organizational structure of the agency, and any function of DIA.

If you are not satisfied with my response to your request, you may contact the DIA FOIA Requester Service Center, as well as our FOIA Public Liaison at 301-394-5587.

Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. You may contact OGIS by email at ogis@nara.gov; telephone at 202-741-5770, toll free at 1-877-684-6448 or facsimile at 202-741-5769; or you may mail them at the following address:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road-OGIS
College Park, MD 20740-6001

You may also exercise your right to file an administrative appeal by writing to the address below and referring to case number 0345-2018. Your appeal must be postmarked no later than 90 days after the date of this letter.

Defense Intelligence Agency
7400 Pentagon
ATTN: FAC-2A1 (FOIA)
Washington, D.C. 20301-7400

Sincerely,

for

Brian L. Jenkins
Chief, Records Management and Information Services

9 Enclosures

What Can You Do? (Continued)

Contracts: CORs and Program Managers must identify effective OPSEC measures and requirements before releasing information into the public domain. When contracts are developed, advertised, negotiated, and implemented, seemingly innocuous but sensitive agency information may be released into the public domain and into corporate channels where it might not be protected without specific OPSEC countermeasures.

Know Your OPSEC PM or Coordinator and Your Critical Information: Integrate OPSEC in your processes and help your designated OPSEC person when asked. Review your current OPSEC measures for appropriateness and adequacy.

Secure Your Data: Sanitize! If you must share information or details, consider how what you post can be aggregated and analyzed to determine vulnerabilities. Sanitize sensitive, critical, and personal information about you, your fellow coworkers, family, and friends from what you post online. Ask yourself 3 questions before posting:

- Why are you sharing this?
- What will people do with this information?
- How will this information be transmitted and stored?

Points of Contact

DIA OPSEC Program Office

(b)(3):10 USC 424

Have a security or counterintelligence report you need to make? (Topics may include but are not limited to: Foreign Travel, Foreign Contact, Unsolicited Contact, Suspicious Activity, Security Incident, or other reports to counterintelligence investigations.)

(b)(3):10 USC 424

Have a general security related question? Contact:

(b)(3):10 USC 424

References

(b)(3):10 USC 424

DSN 3x151

...y (OPSEC)
...tion #5

Contract and Operations Security (OPSEC)

OPSEC:
Use It or Lose It!

Force Protection Branch
Security Operations Division

One Mission, One Team, One Agency

MISSION (b)(3):10 USC 424

What is Operations Security (OPSEC)?

OPSEC is a process used to deny adversaries access to critical information about DIA capabilities, intentions, and operational activities.

Critical Information

Items of OPSEC critical information are specific facts needed by adversaries to plan and perform actions against our missions. A Critical Information List (CIL) should include specifics for the mission of each work center. As CILs are aggregated across multiple mission areas, they become more generalized to keep the size manageable, and serve as memory joggers. Critical information may exist in details relating to:

- **Current/future operations or programs**
- **Organizational capabilities/limitations**
- **Official travel itineraries**
- **Security procedures**
- **Usernames and passwords**
- **Vulnerabilities**

OPSEC should also be applied to personal information, which may help protect you, your fellow employees and your family.

- **Personally Identifiable Information (PII)**
  - **Phone numbers**
  - **Email addresses**
  - **Home, work addresses**
  - **Vehicle information**
  - **Drivers licenses**
  - **Credit card number**
  - **SSN, date/place of birth**
  - **Bank accounts, credit cards**
  - **Biometrics: voice, video, photos**
- **Personal Health Information (PHI)**
  - **Prescriptions**
  - **Allergies**
  - **Medical conditions**
  - **Primary care physicians/locations**

Contracts

The Office of the Acquisition Executive (AE) is responsible for establishing appropriate processes that enforce accountability for, and integration of specific OPSEC requirements within all contracting processes.

Program Managers (PMs), Subject Matter Experts (SMEs), and Contract Representatives (CORs) must be aware of the importance of protecting unclassified critical information associated with contracted activities and must identify, articulate, and include OPSEC requirements in all solicitations, contracts, and resulting Statements of Work (SOW).

DD Form 254

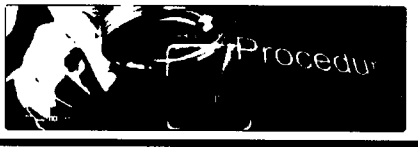
A DD Form 254 must be issued with all contracts which require the storage, handling, or processing of classified information. The DD Form 254 must specify that OPSEC measures are required and identify the need to develop appropriate countermeasures.

Guidance

Contracts which specify OPSEC requirements must include guidance to the contractor in sufficient detail to ensure complete understanding of those OPSEC requirements and the countermeasures.

OPSEC indicators which include friendly detectable actions and open source information which could be interpreted or pieced together by an adversary to derive critical information, must also be protected.

Government directed OPSEC measures may be addressed to any functional process or procedure with the intention of reducing adversarial access to OPSEC indicators or critical information. This is often achieved by eliminating or modifying the indicator.



Minimum Contract Requirements

- The contractor will apply Operations Security (OPSEC) to enhance protection for classified and unclassified critical information.
- When contract performance is at the government site, contractors will comply with OPSEC measures/requirements established by the government.
- When performance is at a contractor site, the contractor PM will appoint an OPSEC coordinator who will:
  - Complete the OPSEC Fundamentals Course (OPSE 1300/1301 or the DSS variant).
  - Maintain a CIL and implement OPSEC.
  - Participate in the review of information the contractor proposed for public release.
  - Maintain records to support compliance inspections.
- All contractors will protect critical information.
- All contractors will receive initial and recurring OPSEC awareness training.

Minimum OPSEC Requirements

- Identify critical information that requires protection.
- Implement countermeasures to eliminate vulnerabilities that create unacceptable risk.
- Ensure personnel are aware of critical information and the directed countermeasures.
- Monitor processes for new vulnerabilities and apply OPSEC.

What Can You Do?

PMs, CORs, OPSEC coordinators, and SMEs must collaborate to ensure the organization's CIL is current and appropriate portions are integrated into contracts. All personnel must apply directed OPSEC countermeasures to protect critical information and be vigilant in reporting OPSEC vulnerabilities.

Can You Do? (Cont

Contracts: CORs and Program Managers must identify effective OPSEC measures and requirements before releasing information into the public domain. When contracts are developed, advertised, negotiated, and implemented, seemingly innocuous but sensitive agency information may be released into the public domain and into corporate channels where it might not be protected without specific OPSEC countermeasures.

Know Your (b)(3):10 USC 424 **nd Your Critical Information:** Integrate OPSEC in your processes and help your designated OPSEC person when asked. Review your current OPSEC measures for appropriateness and adequacy.

Secure Your Data: Sanitize! If you must share information or details, consider how what you post can be aggregated and analyzed to determine vulnerabilities. Sanitize sensitive, critical, and personal information about you, your fellow coworkers, family, and friends from what you post online. Ask yourself 3 questions before posting:

- Why are you sharing this?
- What will people do with this information?
- How will this information be transmitted and stored?

Points of Contact

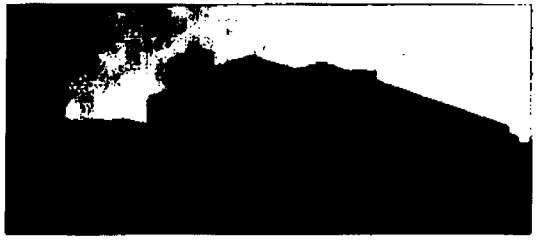
(b)(3):10 USC 424

Have a security or counterintelligence report you need to make? (Topics may include but are not limited to: Foreign Travel, Foreign Contact, Unsolicited Contact, Suspicious Activity, Security Incident, or other reports to) (b)(3):10 USC 4

Use this link or (b)(3):10 USC 424

Have a general security related question? Contact:

(b)(3):10 USC 424



References

(b)(3):10 USC 424

Contracts and Operations Security (OPSEC)

(b)(3):10 USC 424

[redacted] Is Operations Security (OPSEC)

OPSEC is a process used to deny adversaries access to critical information about DIA capabilities, intentions, and operational activities.

Critical Information

Items of OPSEC critical information are specific facts needed by adversaries to plan and perform actions against our missions. A Critical Information List (CIL) should include specifics for the mission of each work center. As CILs are aggregated across multiple mission areas, they become more generalized to keep the size manageable, and serve as memory joggers. Critical information may exist in details relating to:

- Current/future operations or programs
- Organizational capabilities/limitations
- Official travel itineraries
- Security procedures
- Usernames and passwords
- Vulnerabilities

OPSEC should also be applied to personal information, which may help protect you, your fellow employees and your family.

- Personally Identifiable Information (PII)
  - Phone numbers
  - Email addresses
  - Home, work addresses
  - Vehicle information
  - Drivers licenses
  - Credit card number
  - SSN, date/place of birth
  - Bank accounts, credit cards
  - Biometrics: voice, video, photos
- Personal Health Information (PHI)
  - Prescriptions
  - Allergies
  - Medical conditions
  - Primary care physicians/locations

Contracts

The (b)(3):10 USC 424 responsible for establishing appropriate processes that enforce accountability for, and integration of specific OPSEC requirements within all contracting processes.

(b)(3):10 USC 424 must be aware of the importance of protecting unclassified critical information associated with contracted activities and must identify, articulate, and include OPSEC requirements in all solicitations, contracts, and resulting Statements of Work (SOW).

DD Form 254

A DD Form 254 must be issued with all contracts which require the storage, handling, or processing of classified information. The DD Form 254 must specify that OPSEC measures are required and identify the need to develop appropriate countermeasures.

Guidance

Contracts which specify OPSEC requirements must include guidance to the contractor in sufficient detail to ensure complete understanding of those OPSEC requirements and the countermeasures.

OPSEC indicators which include friendly detectable actions and open source information which could be interpreted or pieced together by an adversary to derive critical information, must also be protected.

Government directed OPSEC measures may be addressed to any functional process or procedure with the intention of reducing adversarial access to OPSEC indicators or critical information. This is often achieved by eliminating or modifying the indicator.

Minimum Contract Requirements

- The contractor will apply Operations Security (OPSEC) to enhance protection for classified and unclassified critical information.
- When contract performance is at the government site, contractors will comply with OPSEC measures/requirements established by the government.
- When performance is at a contractor site, the contractor PM will appoint an OPSEC coordinator who will:
  - Complete the OPSEC Fundamentals Course (OPSE 1300/1301 or the DSS variant).
  - Maintain a CIL and implement OPSEC.
  - Participate in the review of information the contractor proposed for public release.
  - Maintain records to support compliance inspections.
- All contractors will protect critical information.
- All contractors will receive initial and recurring OPSEC awareness training.

Minimum OPSEC Requirements

- Identify critical information that requires protection.
- Implement countermeasures to eliminate vulnerabilities that create unacceptable risk.
- Ensure personnel are aware of critical information and the directed countermeasures.
- Monitor processes for new vulnerabilities and apply OPSEC.

What Can You Do?

(b)(3):10 USC 424 must collaborate to ensure the organization's CIL is current and appropriate portions are integrated into contracts. All personnel must apply directed OPSEC countermeasures to protect critical information and be vigilant in reporting OPSEC vulnerabilities.

DIA INCIDENT ALERT

IF YOU ANSWER "YES" TO ANY OF THE FOLLOWING QUESTIONS, YOU MAY HAVE A SECURITY INCIDENT!

- Brought your cellphone, iPod, or laptop into the SCIF?
- Was the last email you sent improperly classified?
- Taken a classified document out of the facility?
- Used the unclassified scanner to upload a classified document onto the network?
- Received an email with an attachment classified higher than the overall classification of the email?
- Participated in a classified conversation outside of a secure area?
- Attended a meeting where unauthorized information was disclosed to foreign partners?
- Received an email containing information that you are not cleared for?

Report all security incidents in CISRS at (b)(3):10 USC 424

DEFENSE INTELLIGENCE AGENCY
COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION

DIA INCIDENT ALERT

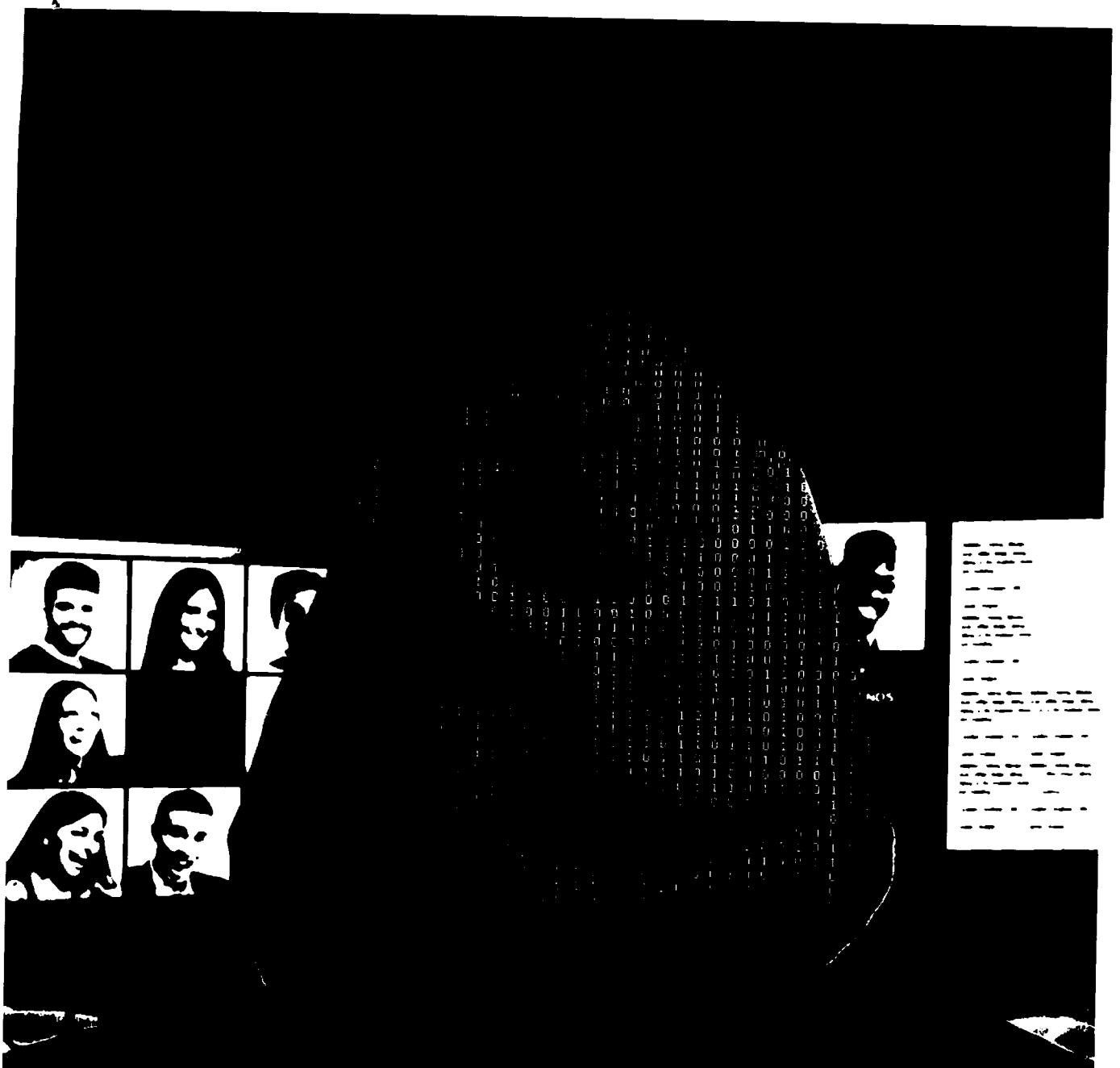
IF YOU ANSWER "YES" TO ANY OF THE FOLLOWING QUESTIONS, YOU MAY HAVE A SECURITY INCIDENT!

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Report all security incidents in CISRS at: (b)(3):10 USC 424

DEFENSE INTELLIGENCE AGENCY

COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION



Your Badge:

Don't leave it in your car.

Put it away when you leave the building.

Report lost badges to security immediately.

FOR MORE INFORMATION CONTACT: (b)(3):10 USC 424

DEFENSE INTELLIGENCE AGENCY

Your Badge:

(b)(3):10 USC 424

DEFENSE INTELLIGENCE AGENCY

OPSEC

What Can You Do? (Continued)

Contracts: CORs and Program Managers must identify effective OPSEC measures and requirements before releasing information into the public domain. When contracts are developed, advertised, negotiated, and implemented, seemingly innocuous but sensitive agency information may be released into the public domain and into corporate channels where it might not be protected without specific OPSEC countermeasures.

Secure Your Data: Sanitize! If you must share information or details, consider how what you post can be aggregated and analyzed to determine vulnerabilities. Sanitize sensitive, critical, and personal information about you, your fellow coworkers, family, and friends from what you post online. Ask yourself 3 questions before posting:

- Why are you sharing this?
- What will people do with this information?
- How will this information be transmitted and stored?

Report Incidents!

Points of Contact

DIA OPSEC Program Office

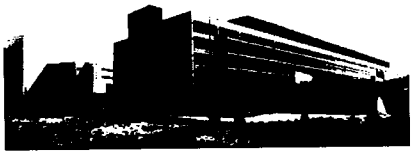
(b)(3):10 USC 424

Have a security or counterintelligence report you need to make? (Topics may include but are not limited to: Foreign Travel, Foreign Contact, Unsolicited Contact, Suspicious Activity, Security Incident, or other reports to counterintelligence investigations.)

(b)(3):10 USC 424

Have a general security related question? Contact:

(b)(3):10 USC 424



References

(b)(3):10 USC 424

...y (OPSEC)
...tion #4

Open Source Intelligence (OSINT) and Operations Security (OPSEC)

OPSEC:
Use It or Lose It!

Force Protection Branch
Security Operations Division

One Mission. One Team. One Agency

MISSION (b)(3):10 USC 424

What is Operations Security (OPSEC)?

OPSEC is a process used to deny adversaries access to critical information about DIA capabilities, intentions, and operational activities.

Critical Information

Items of OPSEC critical information are specific facts needed by adversaries to plan and perform actions against our missions. A Critical Information List (CIL) should include specifics for the mission of each work center. As CILs are aggregated across multiple mission areas, they become more generalized to keep the size manageable, and serve as memory joggers. Critical information may exist in details relating to:

- Current/future operations or programs
- Organizational capabilities/limitations
- Official travel itineraries
- Security procedures
- Usernames and passwords
- Vulnerabilities

OPSEC should also be applied to personal information, which may help protect you, your fellow employees and your family.

- Personally Identifiable Information (PII)
  - Phone numbers
  - Email addresses
  - Home, work addresses
  - Vehicle information
  - Drivers licenses
  - Credit card number
  - SSN, date/place of birth
  - Bank accounts, credit cards
  - Biometrics: voice, video, photos
- Personal Health Information (PHI)
  - Prescriptions
  - Allergies
  - Medical conditions
  - Primary care physicians/locations

Open Source Intelligence (OSINT)

Adversaries collect more than 80 percent of the information they need to derive classified operational details, using unclassified open sources and publicly attained USG materials and information.

Methods adversaries use to collect information include, but are not limited to:

- Reading web pages
- Accessing professional discussion forums
- Joining chat rooms
- Microblogging (Twitter, Identi.ca, Ping.fm)
- Reading personal blogs
- Accessing public job postings and online resumes
- Reviewing government contract offerings
- Joining social networking sites (Facebook/MySpace, etc.)
- Online elicitation
- Telephonic contact using true or false identities
- Phishing and spear phishing techniques
- Analyzing trash discarded at work or home
- Surreptitious access to, or theft of, items during official or personal travel, deployments, or other offsite activities.
- Collecting brochures, pamphlets, business cards, and other publications distributed at USG-sponsored conferences.
- Reviewing publicly available technical manuals, and general information about U.S. military technology.

What Can You Do?

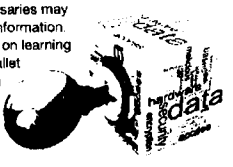
Be Vigilant!

Personal Web Pages, Chat Rooms, and Blogs: Know your audience! Don't post personal information. Apply OPSEC before posting information! When you were a child, you learned the rule, "Don't talk to strangers." When you post information on the Internet, it is available worldwide.

Email: Become "CLICK-SHY!" Review the contents of unencrypted emails before clicking [SEND]. Email can be intercepted or monitored. **Don't click on email attachments or links from unknown sources!** Attachments and links may contain malware and spyware

Conversations and photography in public places: Avoid inappropriate conversations and taking photographs of operational locations that could result in the compromise of critical unclassified or classified information! You may compromise information when taking photographs at operational locations. What content did you inadvertently capture? Additionally, modern digital cameras can record dates and geographic coordinates that can be used by adversaries if intercepted after images are saved, posted, or emailed later.

Travel, Theft, Cyber Capabilities: Protect equipment and information in the physical and online domains. Ensure laptop hard drives are encrypted and when traveling, minimize what you take with you. If operations are planned, apply the OPSEC process before the event and determine your OPSEC measures in advance. In addition to stealing items, many adversaries may temporarily access items or information. Cyber activities often depend on learning details from an unwatched wallet or device, copying or planting information on an electronic device, and performing nefarious activities days or months later.



AWARENESS VIGILANCE SECURE

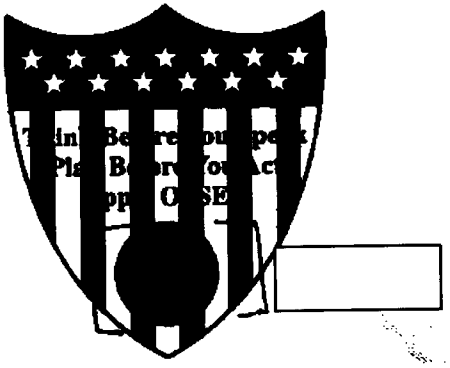
[illegible] Can You Do? (Con[illegible]

Contracts (b)(3):10 USC 424 **must identify effective OPSEC measures and requirements before releasing information into the public domain.** When contracts are developed, advertised, negotiated, and implemented, seemingly innocuous but sensitive agency information may be released into the public domain and into corporate channels where it might not be protected without specific OPSEC countermeasures.

Secure Your Data: Sanitize! If you must share information or details, consider how what you post can be aggregated and analyzed to determine vulnerabilities. Sanitize sensitive, critical, and personal information about you, your fellow coworkers, family, and friends from what you post online. Ask yourself 3 questions before posting:

- Why are you sharing this?
- What will people do with this information?
- How will this information be transmitted and stored?

Report Incidents!



Points of Contact

DIA OPSEC Program Office

(b)(3):10 USC 424

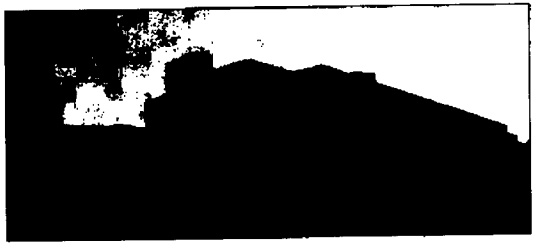
Have a security or counterintelligence report you need to make? (Topics may include but are not limited to: Foreign Travel, Foreign Contact, Unsolicited Contact, Suspicious Activity, Security Incident, or other reports to (b)(3):10 USC 42

(b)(3):10 USC 424

(b)(3):10 USC 424

Have a general security related question? Contact:

(b)(3):10 USC 424



References

(b)(3):10 USC 424

Open Source Intelligence (OSINT) and Operations Security (OPSEC)

(b)(3):10 USC 424

[redacted] Operations Security (OPSEC)

OPSEC is a process used to deny adversaries access to critical information about [redacted] capabilities, intentions, and operational activities.

Critical Information

Items of OPSEC critical information are specific facts needed by adversaries to plan and perform actions against our missions. A Critical Information List (CIL) should include specifics for the mission of each work center. As CILs are aggregated across multiple mission areas, they become more generalized to keep the size manageable, and serve as memory joggers. Critical information may exist in details relating to:

- Current/future operations or programs
- Organizational capabilities/limitations
- Official travel itineraries
- Security procedures
- Usernames and passwords
- Vulnerabilities

OPSEC should also be applied to personal information, which may help protect you, your fellow employees and your family.

- Personally Identifiable Information (PII)
  - Phone numbers
  - Email addresses
  - Home, work addresses
  - Vehicle information
  - Drivers licenses
  - Credit card number
  - SSN, date/place of birth
  - Bank accounts, credit cards
  - Biometrics: voice, video, photos
- Personal Health Information (PHI)
  - Prescriptions
  - Allergies
  - Medical conditions
  - Primary care physicians/locations

Open Source Intelligence (OSINT)

Adversaries collect more than 80 percent of the information they need to derive classified operational details, using unclassified open sources and publicly attained USG materials and information.

Methods adversaries use to collect information include, but are not limited to:

- Reading web pages
- Accessing professional discussion forums
- Joining chat rooms
- Microblogging (Twitter, identi.ca, Ping.fm)
- Reading personal blogs
- Accessing public job postings and online resumes
- Reviewing government contract offerings
- Joining social networking sites (Facebook/MySpace, etc.)
- Online elicitation
- Telephonic contact using true or false identities
- Phishing and spear phishing techniques
- Analyzing trash discarded at work or home
- Surreptitious access to, or theft of, items during official or personal travel, deployments, or other offsite activities.
- Collecting brochures, pamphlets, business cards, and other publications distributed at USG-sponsored conferences.
- Reviewing publicly available technical manuals, and general information about U.S. military technology.

[redacted] What Can You Do?

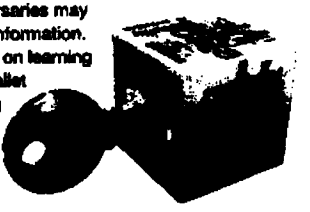
Be Vigilant!

Personal Web Pages, Chat Rooms, and Blogs: Know your audience! Don't post personal information. Apply OPSEC before posting information! When you were a child, you learned the rule, "Don't talk to strangers." When you post information on the Internet, it is available worldwide.

Email: Become "CLICK-SHY!" Review the contents of unencrypted emails before clicking [SEND]. Email can be intercepted or monitored. **Don't click on email attachments or links from unknown sources!** Attachments and links may contain malware and spyware.

Conversations and photography in public places: Avoid inappropriate conversations and taking photographs of operational locations that could result in the compromise of critical unclassified or classified information! You may compromise information when taking photographs at operational locations. What content did you inadvertently capture? Additionally, modern digital cameras can record dates and geographic coordinates that can be used by adversaries if intercepted after images are saved, posted, or emailed later.

Travel, Theft, Cyber Capabilities: Protect equipment and information in the physical and online domains. Ensure laptop hard drives are encrypted and when traveling, minimize what you take with you. If operations are planned, apply the OPSEC process before the event and determine your OPSEC measures in advance. In addition to stealing items, many adversaries may temporarily access items or information. Cyber activities often depend on learning details from an unwatched wallet or device, copying or planting information on an electronic device, and performing nefarious activities days or months later.



Family Members

Did You Know?

Adversaries obtain approximately 80 percent of their intelligence from open sources. Seemingly innocuous details are often just what the adversary needs as he conducts his planning.

Family members of DIA personnel may be aware of some OPSEC critical information without knowing. Generally speaking, critical information includes facts about DIA's intentions, capabilities, operations, or activities that adversaries need in their planning, before conducting missions against DIA personnel or operations.

What Can You Do?

Make an adversary's job more difficult by reducing the availability of details to increase the amount of effort adversaries must perform and the time needed to plan hostile acts. Families can apply OPSEC measures to protect your country and personnel who defend it, whether in DIA or in the military forces we support.

Respect decisions made by your DIA family member regarding sharing of information about work. Help your DIA family member manage risk by not undermining his or her efforts.

Use care when talking, emailing, or texting with other family members, associates, or strangers.

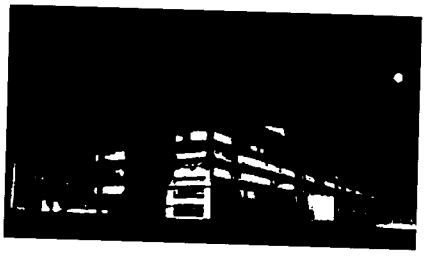
Don't share details that you know about your family member's workplace or work activities. Use discretion in conversations and on personal web pages or social networking sites (SNS). While some protections exist on these sites, the information posted can often be exploited and shared without your knowledge.

OPSEC can be applied to personal, financial, and other private details of your family. Applying OPSEC to your family matters can help reduce the likelihood of being targeted by adversaries. Adversaries can also be local criminals...make yourself and your home a hard target by protecting details that aid criminals.

Points of Contact

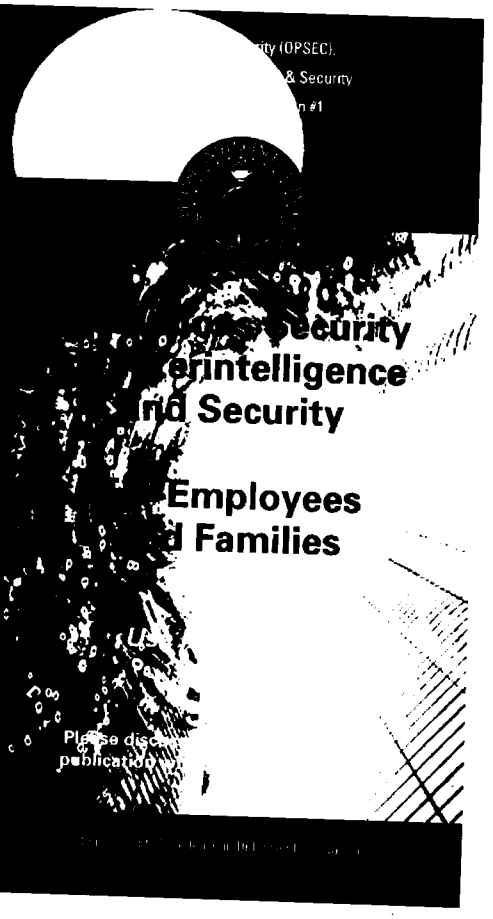
Operations Security (OPSEC), Counterintelligence (CI) & Security

(b)(3):10 USC 424



References

(b)(3):10 USC 424



What is Operations Security (OPSEC)?

OPSEC is a process used to deny adversaries access to critical information about DIA capabilities, intentions, and operational activities. **Critical Information** may exist in details relating to:

- Current and future operations or programs
- Organizational capabilities and limitations
- Travel itineraries
- Security procedures
- Usernames and passwords

OPSEC can also be applied to personal information, which may help protect you, your fellow employees and your family.

Adversaries could collect OPSEC indicators and critical information using various collection techniques.

How Do Adversaries Collect?

Some methods adversaries use to collect information include, but are not limited to:

- Reading web pages, chat rooms, Twitter "tweets," blogs, job postings, contract offerings, online resumes, and social networking sites; and conducting elicitation online or telephonically using true or false identities
- Acquiring data from Portable Electronic Devices (PEDs). PEDs include Personal Digital Assistants (PDAs), cell phones, two-way pagers, smart phones, mobile email devices, digital music storage devices, laptops, tablets, e-readers, and any other devices with networking or wireless capability
- Eavesdropping and surveillance
- Phishing and Spear Phishing
- Analyzing trash and recycling items discarded at work or home

What Can You Do?

Be Vigilant!

Social Media and Blogs: Know your audience! Don't post personal information. Apply OPSEC before giving out or posting information! When you were a child, you learned the rule, "Don't talk to strangers." When you post information on the Internet, it is available worldwide.

Email: Become "CLICK-SHY!" Review the contents of unencrypted emails before clicking [SEND]. Don't click on email attachments or links from unknown sources! Email can be intercepted or monitored. Attachments and links may contain Malware and Spyware.

Wireless Devices: Use the strongest encryption available and a strong password. Avoid using public WIFI hotspots or use VPN when you need to. Privacy is sometimes an illusion, especially overseas. Tools exist today to intercept and collect signals emitting from cellular phones, PEDs, PDAs, personal computers, and Bluetooth headsets. These devices can be an adversary's cheapest agents. Phones and Bluetooth headsets can be converted into active microphones that broadcast to an agent.

Conversations and photography in public places: Avoid inappropriate conversations and taking photographs of operational locations that could result in the compromise of classified information or unclassified critical information! Think before you speak in public areas. You may compromise information when taking photographs at operational locations. What content did you inadvertently capture? Additionally, modern digital cameras can record dates and geographic coordinates that can be used by adversaries if intercepted after images are saved, posted, or emailed later.

Know your sensitivities: DIA and its organizations have critical information lists. Recognize these details and those that place family members at risk. Protect them from unnecessary exposure.

Trash: "Better Shred Than Read!" Seemingly innocuous tidbits of information provide insight regarding intentions, capabilities, providing the who, when, where, and what.

Contracts: CORs and Program Managers must determine any OPSEC measures and requirements before releasing information into the public domain. Apply OPSEC during contract development, advertising, negotiation, and implementation to manage the seemingly innocuous but sensitive agency information that may be released into the public domain inadvertently. Integrate OPSEC requirements in processes and within contracts.

Travel, Theft, Cyber Capabilities: Protect equipment and information in the physical and online domains. Ensure laptop hard drives are encrypted and when traveling, minimize what you take with you. If travel or operations are planned, apply the OPSEC process before the event and determine your OPSEC measures in advance. In addition to stealing items, many adversaries may temporarily access items or information. Cyber activities often depend on learning details from an unwatched wallet or device, copying or planting information on an electronic device, and performing nefarious activities days or months later.

OPSEC AWARENESS

PROTECT YOUR PERSONAL INFORMATION FROM EXPLOITATION

Who
was in your room while you were out?

Don't
leave electronics in your room.

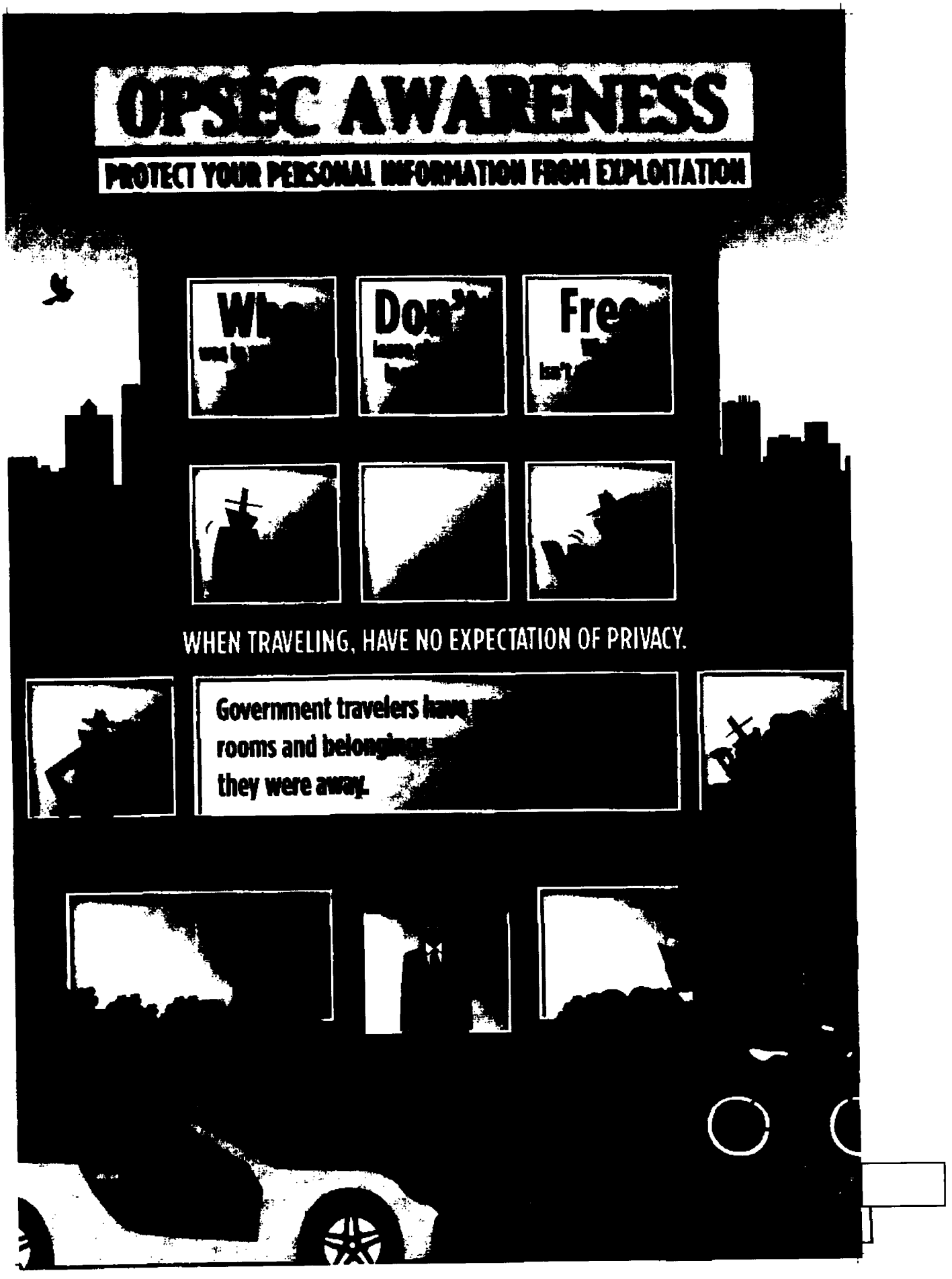
Free
Wi-Fi isn't always free.

WHEN TRAVELING, HAVE NO EXPECTATION OF PRIVACY.

Government travelers have reported their hotel rooms and belongings were searched while they were away.

DEFENSE INTELLIGENCE AGENCY
COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION

(b)(3):10 USC 424


OPSEC AWARENESS
PROTECT YOUR PERSONAL INFORMATION FROM EXPLOITATION
WHEN TRAVELING, HAVE NO EXPECTATION OF PRIVACY.
Government travelers have
rooms and belongings
they were away.

OPSEC

What Can You Do?

Be Responsible and Vigilant!

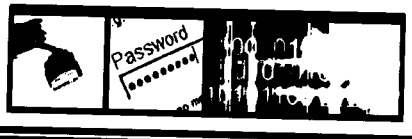
Know Your Device: Know how to operate it properly; Know how and when to disable wireless features. Know how to keep your PED from becoming an unwitting microphone, camera, or transmitter. Operator errors and malicious efforts can lead to devices transmitting conversations or data unintentionally. Disable your PED's wireless functions when not being used.

Secure Your Data: Sanitize and encrypt! If you must travel with your PED, sanitize it of all unnecessary data and always encrypt all remaining data.

Thumbdrives, CDs, and Other Removable Media: Disable Autorun; use security software, don't use media from unknown sources, never connect iPods and other unauthorized devices to government systems. Removable media (USB flash drives, CDs, Memory Sticks, SD Cards, etc.) may include malware. NEVER connect unauthorized media to government systems. Scan authorized media in a stand-alone system.

Content: Use the strongest encryption available, strong passwords, and VPN when you need to discuss or transmit sensitive information. Tools exist to intercept and collect signals emanating from PEDs.

Know What Is Sensitive: Avoid placing sensitive information at risk. Knowing what details are sensitive is a precursor to protecting it. Learn to identify classified and unclassified critical information.



Points of Contact

DIA OPSEC Program Office

(b)(3):10 USC 424

Have a security or counterintelligence report you need to make? (Topics may include but are not limited to: Foreign Travel, Foreign Contact, Unsolicited Contact, Suspicious Activity, Security Incident, or other reports to counterintelligence investigations.)

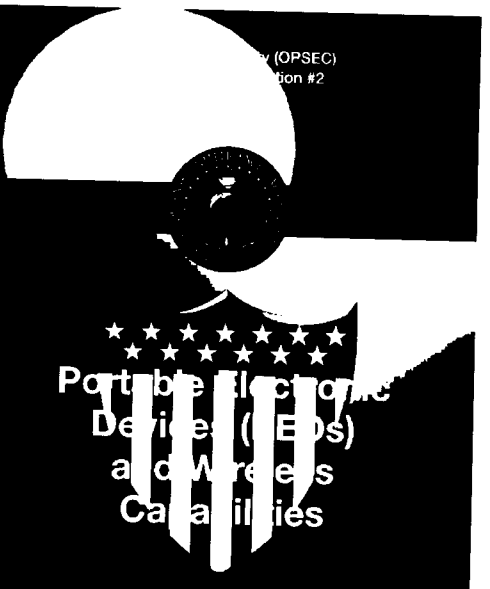
(b)(3):10 USC 424

Have a general security related question? Contact:

(b)(3):10 USC 424

References

(b)(3):10 USC 424



Portable Electronic Devices (PEDs) and Wireless Capabilities

OPSEC:
Use It or Lose It!

Force Protection Branch
Security Operations Division

One Mission. One Team. One Agency.

MISSION (b)(3):10 USC 424

What is Operations Security (OPSEC)?

OPSEC is a process used to deny adversaries access to critical information about DIA capabilities, intentions, and operational activities.

Critical Information may exist in details relating to:

- **Current and future operations or programs**
- **Organizational capabilities and limitations**
- **Travel itineraries**
- **Security procedures**
- **Usernames and passwords**

OPSEC can also be applied to personal information, which may help protect you, your fellow employees, and your family.

OPSEC, PEDs, and Wireless

OPSEC vulnerabilities exist when an adversary can collect indicators and/or critical information and analyze that information to act against DIA.

Portable Electronic Devices (PEDs) include any easily transportable electronic device that has a capability to record, copy, store, and/or transmit data, digital images, video and/or audio.

Wireless internet connectivity is common in a myriad of public and private locations. Wireless connections may create vulnerabilities that adversaries can exploit.

While some OPSEC countermeasures address vulnerabilities that exist in specific situations, all DIA personnel should also apply general OPSEC measures in their daily routines.

This brochure provides general information on some of these measures.

Secure Your Wireless Devices

Here are some simple things you can do to make your information more secure.

Keep operating system and security software updated. This helps prevent intruders from gaining access to your computer.

Use appropriate encryption. Ensure sensitive web traffic is encrypted by checking that the URL begins with "https" and the site has no certificate errors.

Disable or limit folder and printer "sharing" options if you aren't using them.

Use a strong password when accessing a VPN.

Save sensitive files in an encrypted archive file, directory, partition or hard drive that protects sensitive files "at rest."

Use a secure deletion tool to "wipe" temporary copies of sensitive files.

Bluetooth Wireless Capabilities

Adversaries can exploit Bluetooth by conducting eavesdropping, man-in-the-middle and denial of service attacks, and remote operation. General measures to consider include, but are not limited to:

Turn off Bluetooth functionality when not used

Control access to the device

Change the PIN from the default, if possible

Pair the devices indoors and away from windows to reduce options for adversarial collection

Know your equipment and specific vulnerabilities

Travel Considerations

Travel, particularly foreign travel, increases risk that information and PEDs may be vulnerable to adversary exploitation. Consider the following:

Don't advertise your itinerary! Including via email, texts, and any social networking site.

Leave PEDs home! *Don't bring it if you don't need it!* Devices and media may be subject to inspection at airports and when passing through customs inspections. Malware may also be loaded to enable a future exploit.

Securely delete unneeded data and/or restore device to a clean baseline! If you bring PEDs, use tools available to sanitize it and if the Foreign Clearance Guide allows, encrypt remaining data.

Keep operating system and security software current!

Avoid unnecessary activities conducted online!

AWARENESS VIGILANCE SECURE

Portable Electronic Devices (PEDs) and Wireless Capabilities

What Can You Do?

Be Responsible and Vigilant!

Know Your Device: Know how to operate it properly; Know how and when to disable wireless features. Know how to keep your PED from becoming an unwitting microphone, camera, or transmitter. Operator errors and malicious efforts can lead to devices transmitting conversations or data unintentionally. Disable your PED's wireless functions when not being used.

Secure Your Data: Sanitize and encrypt! If you must travel with your PED, sanitize it of all unnecessary data and always encrypt all remaining data.

Thumbdrives, CDs, and Other Removable Media: Disable Autorun; use security software, don't use media from unknown sources, never connect iPods and other unauthorized devices to government systems. Removable media (USB flash drives, CDs, Memory Sticks, SD Cards, etc.) may include malware. NEVER connect unauthorized media to government systems. Scan authorized media in a stand-alone system.

Content: Use the strongest encryption available, strong passwords, and VPN when you need to discuss or transmit sensitive information. Tools exist to intercept and collect signals emanating from PEDs.

Know What is Sensitive: Avoid placing sensitive information at risk. Knowing what details are sensitive is a precursor to protecting it. Learn to identify classified and unclassified critical information.

Points of Contact

(b)(3):10 USC 424

Have a security or counterintelligence report you need to make? (Topics may include but are not limited to: Foreign Travel, Foreign Contact, Unsolicited Contact, Suspicious Activity, Security Incident, or other reports to (b)(3):10 USC 42

(b)(3):10 USC 424

Use this link or (b)(3):10 USC 424

Have a general security related question? Contact:

(b)(3):10 USC 424

References

(b)(3):10 USC 424

(b)(3):10 USC 424

(b)(3):10 USC 424

Operations Security

OPSEC is a process used to deny adversaries access to critical information about DIA capabilities, intentions, and operational activities.

Critical information may exist in details relating to:

- Current and future operations or programs
- Organizational capabilities and limitations
- Travel itineraries
- Security procedures
- Usernames and passwords

OPSEC can also be applied to personal information, which may help protect you, your fellow employees, and your family.

OPSEC, PEDs, and Wireless

OPSEC vulnerabilities exist when an adversary can collect indicators and/or critical information and analyze that information to act against DIA.

Portable Electronic Devices (PEDs) include any easily transportable electronic device that has a capability to record, copy, store, and/or transmit data, digital images, video and/or audio.

Wireless internet connectivity is common in a myriad of public and private locations. Wireless connections may create vulnerabilities that adversaries can exploit.

While some OPSEC countermeasures address vulnerabilities that exist in specific situations, all DIA personnel should also apply general OPSEC measures in their daily routines.

This brochure provides general information on some of these measures.

Secure Your Wireless Devices

Here are some simple things you can do to make your information more secure.

Keep operating system and security software updated. This helps prevent intruders from gaining access to your computer.

Use appropriate encryption. Ensure sensitive web traffic is encrypted by checking that the URL begins with "https" and the site has no certificate errors.

Disable or limit folder and printer "sharing" options if you aren't using them.

Use a strong password when accessing a VPN.

Save sensitive files in an encrypted archive file, directory, partition or hard drive that protects sensitive files "at rest."

Use a secure deletion tool to "wipe" temporary copies of sensitive files.

Bluetooth Wireless Capabilities

Adversaries can exploit Bluetooth by conducting eavesdropping, man-in-the-middle and denial of service attacks, and remote operation. General measures to consider include, but are not limited to:

Turn off Bluetooth functionality when not used

Control access to the device

Change the PIN from the default, if possible

Pair the devices indoors and away from windows to reduce options for adversarial collection

Know your equipment and specific vulnerabilities

Travel Considerations

Travel, particularly foreign travel, increases risk that information and PEDs may be vulnerable to adversary exploitation. Consider the following:

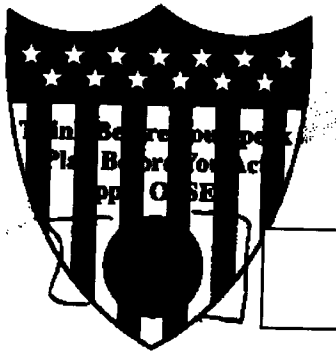
Don't advertise your itinerary! Including via email, texts, and any social networking site.

Leave PEDs home! *Don't bring it if you don't need it!* Devices and media may be subject to inspection at airports and when passing through customs inspections. Malware may also be loaded to enable a future exploit.

Securely delete unneeded data and/or restore device to a clean baseline! If you bring PEDs, use tools available to sanitize it and if the Foreign Clearance Guide allows, encrypt remaining data.

Keep operating system and security software current!

Avoid unnecessary activities conducted online!



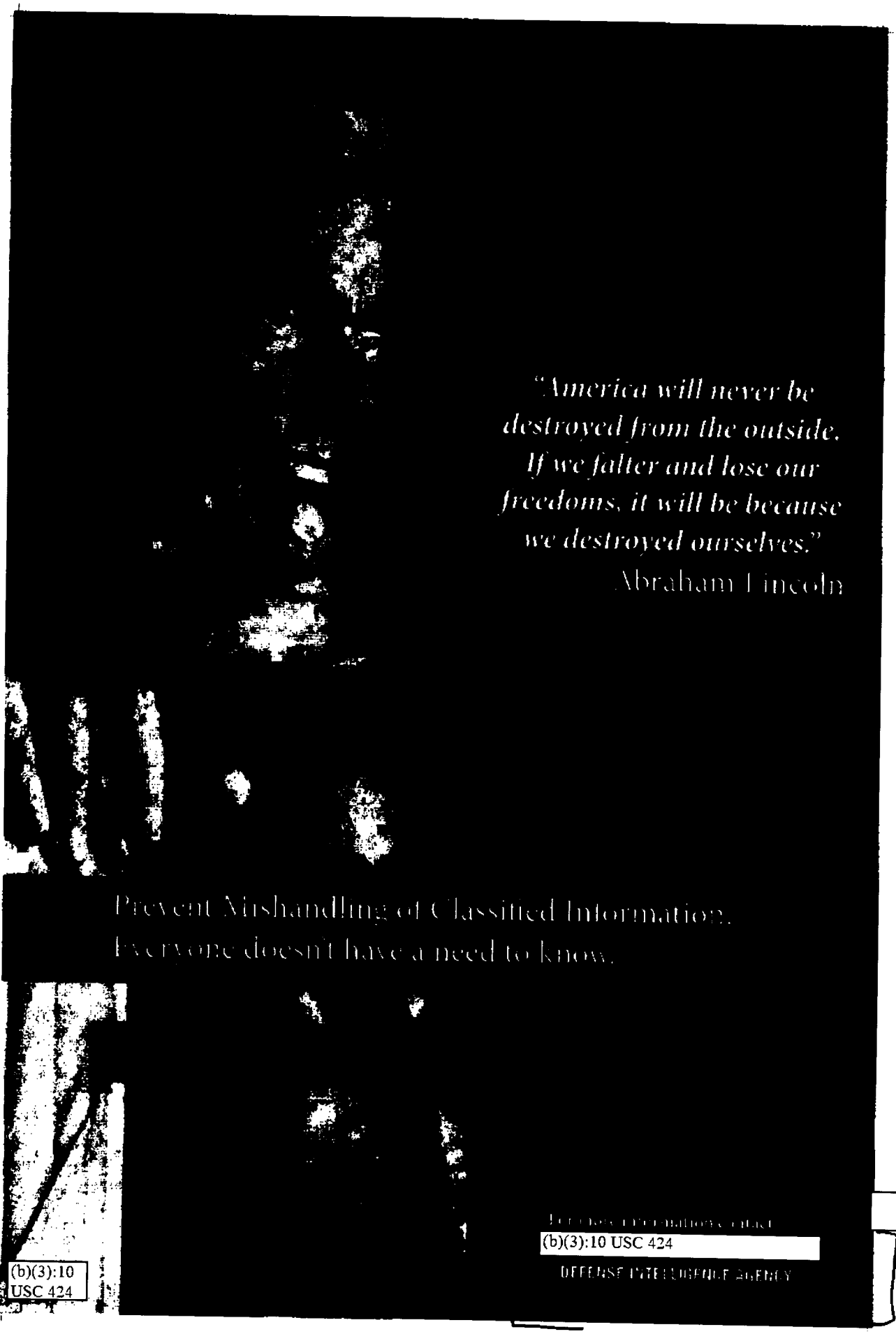
"America will never be destroyed from the outside. If we falter and lose our freedoms, it will be because we destroyed ourselves."

– Abraham Lincoln

Prevent Mishandling of Classified Information.
Everyone doesn't have a need to know.

For more information contact:
(b)(3):10 USC 424

DEFENSE INTELLIGENCE AGENCY


"America will never be destroyed from the outside. If we falter and lose our freedoms, it will be because we destroyed ourselves."
Abraham Lincoln
Prevent Mishandling of Classified Information.
Everyone doesn't have a need to know.
(b)(3):10 USC 424
(b)(3):10 USC 424
DEFENSE INTELLIGENCE AGENCY

What Can You Do?

Know What Is Sensitive: Avoid placing sensitive information at risk! Knowing what details are sensitive is a precursor to protecting it. Learn to identify unclassified critical information. Consult with your organization's OPSEC Coordinator about the critical information list (CIL).

Consider Secure Options First: Use available resources suited towards supporting your mission! Depending on your audience, it could be possible to properly share sensitive information with the right audience using secure resources, such as A-Space, J-Space, secure VoIP phones, and more.

Know Your Exposure: Know where your information is, how it can be accessed by people and who can access it! Social media and social networking sites are designed to share information in different ways. Educate yourself on the design of sites where you maintain an account. Understand how your information is shared. Keep track of online accounts and login credentials. Use a password manager to help manage accounts. Change passwords regularly and ensure that they are not easily guessable.

Secure Your Data: Sanitize! If you must share information or details, consider how what you post can be aggregated and analyzed to determine vulnerabilities. Sanitize sensitive, critical, and personal information about you, your fellow coworkers, family, and friends from what you post online. Ask these three questions before posting:

- Why are you sharing this?
- What will people do with this information?
- How will this information be transmitted and stored?

Report Suspected Incidents: Report if you suspect tampering, phishing, or other anomalous activity! Often, serious activities persisted longer than they would have if people had reported strange behaviors and activities in a timely manner. Apply recommendations in this brochure and be proactive regarding your organization's information security, operations security, and your personal security.

Points of Contact

(b)(3):10 USC 424

Have a security or counterintelligence report you need to make? (Topics may include but are not limited to: Foreign Travel, Foreign Contact, Unsolicited Contact, Suspicious Activity, Security Incident, or other reports to counterintelligence investigations.)

(b)(3):10 USC 424

Have a general security related question? Contact:

(b)(3):10 USC 424

Report Incidents!

If you suspect that you or a family member are being harassed, scammed, or targeted by online malicious activity, it is critical that you capture all relevant information about the incident. Make detailed, chronological notes describing what happened and save any relevant files that help document the incident. It may also help to print copies or take screenshots (*Alt+PrintScreen*) of your view in the browser or other application to illustrate the incident. File a report with proper authorities and attach related documentation.

- DIA Points of Contact (listed above)
- Your Internet Service Provider
- Affected Social Media or Social Networking Site(s)
- Local police
- FBI Internet Crime Complaint Center (*ic3.gov*)

References

(b)(3):10 USC 424

y (OPSEC)
tion #3

S c a Me a and
Oper t or s e urity
(P E C)

OPSEC:
Use It or Lose It!

Force Protection Branch
Security Operations Division

Committed to Excellence in Defense of the Nation

One Mission. One Team. One Agency

MISSION (b)(3):10 USC 424

What is Operations Security (OPSEC)?

OPSEC is a process used to deny adversaries access to critical information about DIA capabilities, intentions, and operational activities.

Critical Information may exist in details relating to:

- **Current/future operations or programs**
- **Organizational capabilities/limitations**
- **Official travel itineraries**
- **Security procedures**
- **Usernames and passwords**
- **Vulnerabilities**

OPSEC should also be applied to personal information, which may help protect you, your fellow employees and your family.

Social Media and OPSEC

Social media includes a range of online capabilities that are increasingly integrated. Social media includes social networking sites (SNS), instant messaging (IM), photo and video sharing, topic-oriented themed sites, and collaborative wikis, among others. They connect people and information in interactive ways. Use of mobile devices (like smart phones and tablets) adds both timeliness and other sensor data, such as geo-location, photographic, and video data to the sites.

Social media are used for recreational sharing, job search, recruiting, advertising, professional networking, and much more. Its use has become mainstream during disasters as a communications tool.

Adversaries can also collect critical information and indicators from social media. Adversaries may include Foreign Intelligence Entities (FIE), terrorist groups, criminals and criminal organizations, and corporate competitors.

Use Operations Security (OPSEC) to help you understand your critical information and indicators that might be generated via social media. Apply OPSEC to consciously manage information and indicators.

Sharing Information

People are sharing more information than ever before about personal activities, relationships, feelings, and perspectives. Social media has enabled increased ability to share, often with a false sense of anonymity. Adversary often collect details via these networks you would normally only share with your friends. Carefully evaluate which personal details should be shared and the ways most proper to share them.

Don't share everything publicly. Use a more targeted approach when sharing information to allow the right groups of people access. For example, unless you are a public figure, your fully detailed resume with employment and education history, phone number, home address, and email address should not be posted to a publicly accessible location. Use sanitized versions that provide *just enough detail* for review by prospective employers. Provide more complete versions to specific employers who express interest.

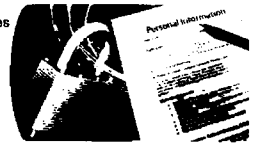
Recommendations

- Read the privacy guides for the social media and social networking sites you use
- Adjust privacy settings on the social networking site and third party applications to protect your identity
- Disable all options, then enable them one by one, as needed; revisit periodically to ensure that they are consistent with your privacy concerns
- Be aware of changes in privacy policies that occur while you are a member of a social networking site
- Use care in who you allow to become your "friend"
- Verify "friends" through alternate means of communication, such as phone or email
- Show the public and "limited friends" a less detailed version of your profile
- Use separate accounts to interact with different audiences: friends and family, business contacts, the public

Personal Information to Protect

Sensitive information also includes your personal information:

- Personally Identifiable Information (PII)
  - Full name
  - Phone numbers
  - Email addresses
  - Home and work addresses
  - Vehicle information
  - Bank accounts
  - Credit card numbers
  - Social Security Number
  - Date and Place of Birth
  - Biometrics: voice, video, photos
- Personal Health Information (PHI)
  - Prescriptions
  - Allergies
  - Medical conditions
  - Primary care physician name and location



What Can You Do?

Know What Is Sensitive: Avoid placing sensitive information at risk! Knowing what details are sensitive is a precursor to protecting it. Learn to identify unclassified critical information. Consult with your organization's (b)(3):10 USC 4 about the critical information list (CIL).

Consider Secure Options First: Use available resources suited towards supporting your mission! Depending on your audience, it could be possible to properly share sensitive information with the right audience using secure resources, such as (b)(3):10 USC 424 and more.

Know Your Exposure: Know where your information is, how it can be accessed by people and who can access it! Social media and social networking sites are designed to share information in different ways. Educate yourself on the design of sites where you maintain an account. Understand how your information is shared. Keep track of online accounts and login credentials. Use a password manager to help manage accounts. Change passwords regularly and ensure that they are not easily guessable.

Secure Your Data: Sanitize! If you must share information or details, consider how what you post can be aggregated and analyzed to determine vulnerabilities. Sanitize sensitive, critical, and personal information about you, your fellow coworkers, family, and friends from what you post online. Ask these three questions before posting:

- Why are you sharing this?
- What will people do with this information?
- How will this information be transmitted and stored?

Report Suspected Incidents: Report if you suspect tampering, phishing, or other anomalous activity! Often, serious activities persisted longer than they would have if people had reported strange behaviors and activities in a timely manner. Apply recommendations in this brochure and be proactive regarding your organization's information security, operations security, and your personal security.

Points of Contact

DIA OPSEC Program Office

(b)(3):10 USC 424

Have a security or counterintelligence report you need to make? (Topics may include but are not limited to: Foreign Travel, Foreign Contact, Unsolicited Contact, Suspicious Activity, Security Incident, or other reports to counterintelligence investigations.)

Use this link or (b)(3):10 USC 424

Have a general security related question? Contact:

(b)(3):10 USC 424

Report Incidents!

If you suspect that you or a family member are being harassed, scammed, or targeted by online malicious activity, it is critical that you capture all relevant information about the incident. Make detailed, chronological notes describing what happened and save any relevant files that help document the incident. It may also help to print copies or take screenshots (*Alt+PrintScreen*) of your view in the browser or other application to illustrate the incident. File a report with proper authorities and attach related documentation.

- DIA Points of Contact (listed above)
- Your Internet Service Provider
- Affected Social Media or Social Networking Site(s)
- Local police
- FBI Internet Crime Complaint Center (*ic3.gov*)

References

(b)(3):10 USC 424

Social Media and Operations Security (OPSEC)

ALL REDACTIONS Based on (3)(b)(9)(1)

(b)(3):10 USC 424

Operations Security (OPSEC)

OPSEC is a process used to deny adversaries access to critical information about DIA capabilities, intentions, and operational activities.

Critical information may exist in details relating to:

- Current/future operations or programs
- Organizational capabilities/limitations
- Official travel itineraries
- Security procedures
- Usernames and passwords
- Vulnerabilities

OPSEC should also be applied to personal information, which may help protect you, your fellow employees and your family.

Social Media and OPSEC

Social media includes a range of online capabilities that are increasingly integrated. Social media includes social networking sites (SNS), instant messaging (IM), photo and video sharing, topic-oriented themed sites, and collaborative wikis, among others. They connect people and information in interactive ways. Use of mobile devices (like smart phones and tablets) adds both timeliness and other sensor data, such as geo-location, photographic, and video data to the sites.

Social media are used for recreational sharing, job search, recruiting, advertising, professional networking, and much more. Its use has become mainstream during disasters as a communications tool.

Adversaries can also collect critical information and indicators from social media. Adversaries may include Foreign Intelligence Entities (FIE), terrorist groups, criminals and criminal organizations, and corporate competitors.

Use Operations Security (OPSEC) to help you understand your critical information and indicators that might be generated via social media. Apply OPSEC to consciously manage information and indicators.

Sharing Information

People are sharing more information than ever before about personal activities, relationships, feelings, and perspectives. Social media has enabled increased ability to share, often with a false sense of anonymity. Adversary often collect details via these networks you would normally only share with your friends. Carefully evaluate which personal details should be shared and the ways most proper to share them.

Don't share everything publicly. Use a more targeted approach when sharing information to allow the right groups of people access. For example, unless you are a public figure, your fully detailed resume with employment and education history, phone number, home address, and email address should not be posted to a publicly accessible location. Use sanitized versions that provide *just enough detail* for review by prospective employers. Provide more complete versions to specific employers who express interest.

Recommendations

- Read the privacy guides for the social media and social networking sites you use
- Adjust privacy settings on the social networking site and third party applications to protect your identity
- Disable all options, then enable them one by one, as needed; revisit periodically to ensure that they are consistent with your privacy concerns
- Be aware of changes in privacy policies that occur while you are a member of a social networking site
- Use care in who you allow to become your "friend"
- Verify "friends" through alternate means of communication, such as phone or email
- Show the public and "limited friends" a less detailed version of your profile
- Use separate accounts to interact with different audiences: friends and family, business contacts, the public

Sensitive Information to Protect

Sensitive information also includes your personal information:

- Personally Identifiable Information (PII)
  - Full name
  - Phone numbers
  - Email addresses
  - Home and work addresses
  - Vehicle information
  - Bank accounts
  - Credit card numbers
  - Social Security Number
  - Date and Place of Birth
  - Biometrics: voice, video, photos
- Personal Health Information (PHI)
  - Prescriptions
  - Allergies
  - Medical conditions
  - Primary care physician name and location